UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/091,735	06/24/1998	IAN DUNCAN BRAMHILL	36-1230	5276

7590   06/28/2004

NIXON & VANDERHYE
1100 NORTH GLEBE ROAD
8TH FLOOR
ARLINGTON, VA 222014714

EXAMINER
NGUYEN, CUONG H

ART UNIT	PAPER NUMBER
3625	

DATE MAILED: 06/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

BEFORE THE BOARD OF PATENT APPEALS AND

INTERFERENCES

Paper No. 22

Application Number: 09/091,735
Filing date: 06/24/1998
Appellants: BRAMHILL et al.

Raymond Mah
For Appellants

MAILED

JUN 2 8 2004

EXAMINER'S ANSWER

GROUP 3600

This is in response to appellants' brief on appeal filed on December 01, 2003.

(1) *Real Party in Interest*

A statement identifying the real party in interest is contained in the brief.

(2) *Related Appeals and Interferences*

There is none related appeal and interference which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) *Status of Claims*

The statement of the status of claims contained in the brief is correct.

(4)   Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5)   *Summary of Invention*

The summary of invention contained in the brief is correct.

(6)   Issues

The appellant's statement of the issues in the brief is correct.

(7)   Grouping of Claims

- Appellant's brief includes a statement that:
- Group I: claims 1-8, 12, 14-18, 21, 28-29, 31-32, 34-35, and 37-38 stand or fall together.
- Group II: claims 30, 33, and 36 stand or fall together; and provides reasons as set forth in 37 CFR

1.192(c)(7) and (c)(8); therefore, claim 34 is taken as a representative of Group I, and claim 36 is taken as a representative of Group II.

(8)   *Claims Appealed*

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9)   Prior Art of Record

The following is a listing of the prior art of record relied upon in the rejection of claims under appeal.

-      Spies et al. (US Pat. 6,055,314),

-      Rhoads (US Pat. 5,841,978).

-      Probst (US Pat. 5,982,899).

-      Crawford (US Pat. 6,014,651).

(10)   Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims. The ground(s) for rejection (for pending claims 1-8, 12, 14-18, 21, 28-38) are reproduced below from the final Office Action and are provided here for the convenience of both Appellants and the Board of Patent Appeals.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11.   Re. to claims 30-38, 1-2, 5-8, 12, 14, 28: They are rejected under 35 U.S.C. §103(a) as being unpatentable over **Spies** et al. (US Pat. 6,055,314).

A. Re. to claim 34: **Spies** et al. teach a method of controlling access to data downloaded from a server computer to a client computer (see Spies et al., 11:22-25), comprising steps of:

- downloading a protected copy of a requested data from a server to a client (see **Spies** et al., 3:36-47, 17:40-45); and

Although Spies et al. do not expressly disclose about - running a program at the client (please note that executing a program for "an entire process" including "after accessing")- this is obviously done by Spies et al. to perform steps of (a) unprotected the download data, and (b) suppress/prevent client computer from copying that unprotected data (see **Spies** et al., 1:47-49, 11:12-15, and 16:55-60).

It would have been obvious to one of ordinary skill in the art at the time of invention that **Spies** et al.'s teachings provide sufficient teaching of "running a program at the client after accessing" because Spies et al.'s steps also for controlling access to data downloaded from a server computer to a client computer.

B. Re. to claim 36: **Spies** et al. teach a method of controlling access to data downloaded from a server computer to a client computer (see Spies et al., 11:22-25), comprising steps of:

- selecting downloaded data (see **Spies** et al., 3:36-38 specifying "ordered data");

- downloading said protected data from a server to a client (see **Spies** et al., 3:36-47, 17:40-45); and

Although Spies et al. do not expressly disclose about "running a program at the client after access is permitted" this is obviously done by Spies et al. to perform steps of using a decryption key to unprotect data and preventing a copy function above. (please note that executing a program for "an entire process" including "after accessing")- this is obviously done by Spies et al. to perform steps of (a) unprotected the download data, and (b) suppress/prevent client computer from copying that unprotected data (see **Spies** et al., 1:47-49, 11:12-15, and 16:55-60).

It would have been obvious to one of ordinary skill in the art at the time of invention that **Spies** et al.'s teachings provide sufficient teaching of "running a program at the client after accessing is permitted" because Spies et al.'s steps also having permissions for controlling access to data downloaded from a server computer to a client computer.

C. Re. to claims 31-32, 35, 37-38: The applicant admits that they contain similar limitations as in rejected claim 34; therefore, similar rationales and reference set forth for 35 USC §103(a) rejections are applied.

D. Re. to claims 30, 33: The applicant admits that they contain similar limitations as in rejected claim 36; therefore, similar rationales and reference set forth for 35 USC §103(a) rejections are applied.

E. Re. To claims 1, 28: The examiner submits that they contain limitations as in rejected claim 31; therefore, similar rationales and reference set forth for 35 USC §103(a) rejections are applied.

F. As per claim 2: The rationales & references for rejection of claim 1 are incorporated.

Spies et al. suggest a method that using encrypted data (see Spies, 16:55-64); the examiner submits that it is equivalent for "data protection" by encrypting.

G. Re. to claims 3-4: The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. also suggest a method that including a hashing algorithm for protecting data integrity (see Spies et al., 7:31-35).

Because protecting crypto graphical data is also a form of protecting data (because both of them are merely data), and protecting crypto graphical data as claimed is analogous of protecting specific data); therefore, it is obvious for one with ordinary skill in the art to use Spies et al.'s teachings to perform a common step of protecting original data.

H. As per claim 5: The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. suggest a step of checking a destination/receiver/client before sending data (see **Spies,** claim 16).

I. As per claim 6: The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. suggest identifying a destination/ receiver/client to a server before sending data (see **Spies,** claim 16); the examiner submits that this has been old, and well-known for artisan to identifying a receiver before sending anything to ensure a safety and correct transaction.

J. As per claim 12: The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. suggest that data are sent to a client through a network (see **Spies et al.,** Fig. 9, 11:22-25); the examiner submits that this has been old, and well-known for sending data via Internet.

K. As per claim 7: The rationales & reference for rejection of claim 1 are incorporated.

The rationales & reference for rejection of claim 1 are incorporated.

Spies et al. obviously suggest:

- generating a program at a server (note: "a program" can be broadly interpreted as any general instruction/data);

- downloading said program to a client, and

   - said client running said program to make a request.

   These above limitations are obviously suggested in **Spies**, 16:19-40 & claim 11.

   The examiner also submits that as a common practice, a server would distribute an available "template"/(program to request a particular software), then a user/client would enter a user/requester's name/address; name/ID of a specific software he needs and uploading those data to the server, those steps has been happening before this application's priority date.

L. As per claim 8: The rationales & reference for rejection of claim 7 are incorporated.

   Spies et al. also obviously suggest that a program/instruction is generated in response to a request for access to a specific data (see **Spies** et al., 16:20-39).

M. As per claim 14: The rationales & reference for rejection of claim 7 are incorporated.

   Spies et al. obviously suggest said program includes data concerning a cryptographic key, using said key to unprotect download data (see **Spies**, 16:19-54).

N.   Claims 3-4, 16 are rejected under 35 U.S.C. §103(a) as being unpatentable over **Spies** et al. (US Pat. 6,055,314), in view of **Rhoads** (US Pat. 5,841,978).

a. As per claim 3: The rationales & reference for rejection of claim 1 are incorporated.

In addition to **Spies** et al.'s protecting any change to original data; **Rhoads** (US Pat. 5,841,978) also discloses a method that comprises protecting an integrity of data (e.g., see **Rhoads,** 57:5-35); please note that this analogous feature to claim 3 has been old, and well-known (e.g. data hashing technique, check-sum technique etc.).

Because protecting crypto graphical data is also a form of protecting data (because both of them are merely data, and protecting crypto graphical data as claimed is analogous of protecting specific data); therefore, it is obvious for one with ordinary skill in the art to combine Spies et al. and Rhoads to protect the integrity of the data cryptographically.

b. As per claim 4: The rationales & reference for rejection of claim 3 are incorporated.

Spies et al. also suggest a method that including a hashing algorithm for data integrity (see **Spies et al.,** 7:31-35); the examiner submits that this has been old, and well-known for hashing data.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine ideas of **Rhoads** & **Spies** et al. to suggest above claimed steps because it

would simply prevent any un-wanted change to original data;

that serves a purpose for preventing original data.

c. As per claim 16:

The rationales & reference for rejection of claim 1 are

incorporated.

Spies et al. do not disclose about using stegano-

graphical data.

However, to implement **Spies et al.**'s invention, **Rhoads'**

patent gave ideas of utilizing stegano-graphical data (see

Rhoads, claim 1).

It would have been obvious to one of ordinary skill in

the art at the time of invention to have incorporated

Rhoads' suggestion to **Spies** invention to suggest claimed

step because it would use an available form of data such as

stegano-graphic marked data for data protection purposes.

O. As per claim 15: This claim is rejected under 35 U.S.C.

§103(a) as being unpatentable over **Spies** et al. (US Pat.

6,055,314), in view of **Probst** (US Pat. 5,982,899).

The rationales & reference for rejection of claim 1 are

incorporated.

Probst suggests what Spies 's missing in claim 15; he

teaches a server and a client each hold data corresponding

to a cryptographic key and a machine identifier for uniquely

identifying a user/client, comprising:

- sending a challenge/query to a user/client (this feature is very well-known), such that it generates a signed response as a cryptographic function of the key and the machine identifier held therein (**Probst** suggests an analogous action for generating a combination feature of a key and a machine identifier, see **Probst,** the abstract),

- generating from the cryptographic key and machine identifier held associated with the server, a corresponding signed response as a cryptographic function of the key and the machine identifier (see **Probst,** the abstract, & 3:8-21 for suggesting a unique identifier by combining a key and a machine identifier);

- comparing the signed responses from the user/client and the server, performing the cryptographic protection of the data with the key (see **Probst,** 4:20-22, claims 5 and 15);

- converting/decrypting protected data into an unprotected form (see **Probst,** the abstract, claims 1, 15, and 3:8-21).

It would have been obvious to one of ordinary skill in the art at the time of invention to have incorporated **Probst's** suggestions to **Spies** invention to suggest above claimed steps because these are necessary and reasonable steps to verify a client by a server before deliver protected data.

P. As per claim 17: This claim is rejected under 35 U.S.C.
§103(a) as being unpatentable over **Spies** et al. (US Pat.
6,055,314), in view of the Official Notice.
The rationales & references for rejection of claim 1 are
incorporated.

Claim 17 contains a step of registering a client with a
server.

The Official Notice is taken that in software renting
business involving server/client (using Internet), a step of
registering a client with a server has been old, & well-
known for logging client identification as a record of each
transaction.

It would have been obvious to one of ordinary skill in
the art at the time of invention to combine above Official
Notice to **Spies** invention to suggest a step of registering a
client with a server because it is a record to verify a
client by a server before deliver protected data.

Q. As per claim 18: This claim is rejected under 35 U.S.C.
§103(a) as being unpatentable over **Spies** et al. (US Pat.
6,055,314), in view of **Crawford** (US Pat. 6,014,651).

The rationales & reference for rejection of claim 1 are
incorporated.

Spies et al. suggest a method that:

- determining a user/client's machine identifier by
hardware configuration, then transmitting said identifier to

a server (see **Spies,** claim 15); the examiner submits that this step has been done prior to this pending invention.

In addition of **Spies et al.**'s patent, **Crawford's** patent also further gave an example for "combining an identifier with a content":

- combining an identifier with a key to form a unique identifier/determinator (see **Crawford,** claim15 wherein the act of combining is represented by a step of encrypting data with customer's identity, and providing said encrypted data);

- transmitting a (unique) identifier/determinator to the client for use (e.g., for identifying/transmitting data etc.)(note: transmitting a specific data to someone on Internet is old and well-known, and this step of transmitting data was done by both Spies et al. and Crawford).

It would have been obvious to one of ordinary skill in the art at the time of invention to have incorporated **Crawford's** suggestion to **Spies** et al. invention to suggest above claimed steps because using a unique identifier is convenient for data protection purposes.

R. As per claims 21, 28: The examiner submits that they contain analogous limitations as claim 31; therefore, similar rationales and reference set forth for 35 USC 103(a) rejection of claim 31 are applied.

(12) Response to Argument:

A.   At first, pending claims difference compared to cited prior art are only found in the non-functional data stored on the article of manufacture. Data identifying a name of a customer, or an image of a customer, or a list of customer's name are not functionally related to the claimed equipment because these descriptive materials will not distinguish the claimed invention from the prior art in terms of patentability, see In re **Gullack**, 703 F.2d 1381, 1385, 217 USPQ 401, 404, (Fed. Cir. 1983); In re **Lowry**, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994).

B.   Spies et al. teach of controlling access to copy and save functions at the client in respect of data in its unprotected form (see Spies et al., 16:55-60); in another word, "prevent copying data one decrypted" were suggested by Spies et al. in 1:47-59, 11:12-15, and 16:55-60 - video data are securely distributed to a set-top-box (STB), where output data from a set-top-box STB to a TV are prevented from copying (please note that Spies teaches controlling access including restricting/preventing task).

C.   On page 8, para.1-2 of the "Appeal Brief" (faxed on 3/29/2004) applicant's arguments about "control, restrict, or prevent … unauthorized access to already decrypted data"
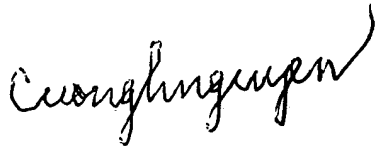
are clearly suggested by Spies et al. (16: 55-60, and 1:47-49).

D.   On page 9, para.1 of the "Appeal Brief" (faxed on 3/29/2004) applicant's arguments about Spies et al.'s teach different environment – a videocassette or a DVD –, the examiner submits that those are exemplary situations as suggested in Spies et al., 1:45-49; however, Spies et al., also teach the environment that is recited in the pending claims (see Spies et al., 11:22-25).

E.   For the argument on page 9, para. 3 to page 10, para.1 of the "Appeal Brief" (faxed on 3/29/2004), although not expressly disclose about "running a program", Spies et al. inherently "running a program" to do downloading and decrypting data (see Spies et al., 2:54-61, and 10:59-67) because commands and controls for using downloaded data MUST be performed by "running a program". About the applicant's argument of "a program portion", this "program portion" is not part of claim 34's limitation, or claim 36's limitation (which represents for Group I or Group II claims).

For the above reasons, it is believed that the rejections should be sustained.
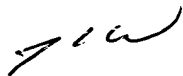
Respectfully submitted,

Cuonghnguyen

Cuong H. Nguyen
June 10, 2004

An appeal conference was held on May 24, 2004 with:

Acting SPE Jeff. A. Smith, Art Unit 3625

SPE John Weiss (Appeal Conference Specialist)

Raymond Mah
1100 N. GLEBE ROAD, 8TH FLOOR
ARLINGTON, VA 22201-4714